Finite Fields and Their Applications 15 (2009) 428–440

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On the Carlitz rank of permutation polynomials

Esen Aksoy, Ayça Çeşmelioğlu [1], Wilfried Meidl, Alev Topuzoğlu *

Sabancı University, Orhanlı, 34956 Tuzla, İstanbul, Turkey

ARTICLE INFO

Article history:
Received 18 March 2008
Revised 27 October 2008
Available online 17 March 2009
Communicated by Rudolf Lidl

Keywords:
Permutation polynomials of finite fields
Carlitz rank
Enumeration of permutation polynomials
Stirling numbers of the first kind

ABSTRACT

A well-known result of Carlitz, that any permutation polynomial $\wp(x)$ of a finite field $\mathbb{F}_q$ is a composition of linear polynomials and the monomial x^{q-2}, implies that $\wp(x)$ can be represented by a polynomial $\mathcal{P}_n(x) = (\cdots((a_0x+a_1)^{q-2}+a_2)^{q-2}\cdots+a_n)^{q-2}+a_{n+1}$, for some $n \geqslant 0$. The smallest integer n, such that $\mathcal{P}_n(x)$ represents $\wp(x)$ is of interest since it is the least number of "*inversions*" x^{q-2}, needed to obtain $\wp(x)$. We define the *Carlitz rank* of $\wp(x)$ as n, and focus here on the problem of evaluating it. We also obtain results on the enumeration of permutations of $\mathbb{F}_q$ with a fixed Carlitz rank.

1. Introduction

Let $\mathbb{F}_q$ be the finite field with $q = p^r$ elements, where p is an odd prime, and $r \geqslant 1$.

By a classical result of Carlitz [1], S_q, the symmetric group on q letters, which is isomorphic to the group of permutation polynomials of $\mathbb{F}_q$ of degree less than $q-1$ under the operation of composition and reduction modulo $x^q - x$, is generated by the linear polynomials $ax+b$, for $a, b \in \mathbb{F}_q$, $a \neq 0$, and x^{q-2} (see [5,6] for a detailed exposition of permutation polynomials of finite fields). Consequently, as pointed out in [3], with $\mathcal{P}_0(x) = a_0x + a_1$, any permutation of a finite field $\mathbb{F}_q$ can be represented by a polynomial

$$\mathcal{P}_n(x) = \left(\cdots\left((a_0x+a_1)^{q-2}+a_2\right)^{q-2}\cdots+a_n\right)^{q-2}+a_{n+1}, \quad n \geqslant 0, \tag{1}$$

* Corresponding author.
E-mail addresses: eaksoy@su.sabanciuniv.edu (E. Aksoy), cesmelioglu@su.sabanciuniv.edu (A. Çeşmelioğlu), wmeidl@sabanciuniv.edu (W. Meidl), alev@sabanciuniv.edu (A. Topuzoğlu).
[1] Ayça Çeşmelioğlu is a recipient of Yousef Jameel scholarship.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2009.02.006

where $a_1, a_{n+1} \in \mathbb{F}_q$, $a_i \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ for $i = 0, 2, \ldots, n$. We follow the notation of [3] and put $\mathcal{P}_n = P_n$ when $a_{n+1} = 0$, i.e.

$$P_n(x) = x^{q-2} \circ (x + a_n) \circ x^{q-2} \cdots x^{q-2} \circ (x + a_2) \circ x^{q-2} \circ (a_0 x + a_1). \tag{2}$$

In case $a_{n+1} \neq 0$ we write $\mathcal{P}_n = \bar{P}_n$, i.e.

$$\bar{P}_n(x) = (x + a_{n+1}) \circ P_n. \tag{3}$$

Obviously n is the number of times x^{q-2} occurs in (2) or (3).

For the polynomial $\mathcal{P}_n(x)$ we consider the function

$$\big(\cdots\big((a_0 x + a_1)^{-1} + a_2\big)^{-1} \cdots + a_n\big)^{-1} + a_{n+1}$$

and its continued fraction expansion,

$$a_{n+1} + 1/\big(a_n + 1/\big(\cdots + a_2 + 1/(a_0 x + a_1)\cdots\big)\big),$$

so as to form the nth *convergent*

$$\mathcal{R}_n(x) = \frac{\alpha_{n+1} x + \beta_{n+1}}{\alpha_n x + \beta_n}, \tag{4}$$

where

$$\alpha_k = a_k \alpha_{k-1} + \alpha_{k-2} \quad \text{and} \quad \beta_k = a_k \beta_{k-1} + \beta_{k-2}, \tag{5}$$

for $k \geqslant 2$ and $\alpha_0 = 0$, $\alpha_1 = a_0$, $\beta_0 = 1$, $\beta_1 = a_1$. Note that α_k and β_k cannot both be zero.

We remark that $\alpha_{n+1} = \alpha_{n-1}$ and $\beta_{n+1} = \beta_{n-1}$ if $a_{n+1} = 0$ and thus $\mathcal{R}_n$ reduces to $(\alpha_{n-1} x + \beta_{n-1})/(\alpha_n x + \beta_n)$. We define the set of *poles*, $\mathbf{O}_n$, as

$$\mathbf{O}_n = \left\{ x_i \colon\ x_i = \frac{-\beta_i}{\alpha_i},\ i = 1, \ldots, n \right\} \subset \mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}. \tag{6}$$

Obviously $\mathcal{P}_n(x) = \mathcal{R}_n(x)$ for $x \in \mathbb{F}_q \setminus \mathbf{O}_n$. Since the ordering and repetition of the poles will be crucial, we will also have to consider the *string of poles* $\mathcal{O}_n$:

$$\mathcal{O}_n = x_1, x_2, \ldots, x_n.$$

To every rational transformation $\mathcal{R}_n(x)$ of the form (4) we can naturally associate a permutation $\mathcal{F}_n(x)$ defined by $\mathcal{F}_n(x) = \mathcal{R}_n(x)$ for $x \neq x_n$ and $\mathcal{F}_n(x_n) = \alpha_{n+1}/\alpha_n$ when $x_n \in \mathbb{F}_q$.

It turns out to be convenient to treat the cases $a_{n+1} = 0$ and $a_{n+1} \neq 0$ separately at times, accordingly we put $\mathcal{R}_n(x) = R_n(x)$, $\mathcal{F}_n(x) = F_n(x)$ for $a_{n+1} = 0$ and $\mathcal{R}_n(x) = \bar{R}_n(x)$, $\mathcal{F}_n(x) = \bar{F}_n(x)$ for $a_{n+1} \neq 0$.

When the poles are distinct elements of $\mathbb{F}_q$, the permutation $\mathcal{P}_n$ is the product of the n-cycle $(\mathcal{F}_n(x_n)\mathcal{F}_n(x_{n-1}) \cdots \mathcal{F}_n(x_1))$ with the permutation $\mathcal{F}_n$, i.e.

$$\mathcal{P}_n(x) = \big(\mathcal{F}_n(x_n)\mathcal{F}_n(x_{n-1}) \cdots \mathcal{F}_n(x_1)\big)\mathcal{F}_n(x) \tag{7}$$

(multiplying in right-to-left order) (see Lemma 1 in [3]).

Results on the cycle structure of $\mathcal{P}_n$ have been presented in [3]. The number of permutations of the form $\mathcal{P}_n$ with a full cycle has been determined in [4] for $n = 1, 2, 3$. Given a permutation $\wp(x)$ of $\mathbb{F}_q$, as is mentioned above, one can find a representation of $\wp(x)$ in terms of $\mathcal{P}_n$ for some $n \geqslant 0$,

where of course, n is not necessarily minimal. We therefore define the *Carlitz rank* of $\wp(x)$, to be the smallest n satisfying $\wp = \mathcal{P}_n$ for a permutation $\mathcal{P}_n$ of the form (1), i.e. $\wp(x)$ is composed of at least n "*inversions*" x^{q-2} with n (or $n+1$) linear polynomials. We denote the Carlitz rank of $\wp(x)$ by $\mathrm{Crk}(\wp)$.

Section 2 of this work focuses on the problem of determining the Carlitz rank of a permutation. For a given permutation $\mathcal{P}_s(x)$ of the form (1), we present a procedure to find a representation $\mathcal{P}_n(x)$ satisfying $\mathcal{P}_s(x) = \mathcal{P}_n(x)$, $n \leqslant s$. Theorem 3 shows how to calculate n and that n is the Carlitz rank of $\mathcal{P}_s$ if $n < (q-1)/2$.

Two main results concerning Carlitz rank are presented in Section 3.

We show in Theorem 4 that small polynomial degree implies large Carlitz rank. More precisely, $\mathrm{Crk}(g) \geqslant q - 1 - d$ if $g(x)$ is a permutation polynomial in $\mathbb{F}_q[x]$ of degree d.

The problem of enumerating permutation polynomials of a given degree is open. Here we tackle the problem of enumerating permutation polynomials of a given Carlitz rank and show in Theorem 5 that the number $\mathcal{B}(n)$ of permutations of $\mathbb{F}_q$ with Carlitz rank n is

$$\begin{aligned}\mathcal{B}(n) = {} & \left(q^2-q\right) \sum_{m=1}^{\lfloor \frac{n+1}{3} \rfloor} \binom{q}{n+1-m} \mathcal{S}(2, n+1-m, m)(n+1-m) \\ & + \left(q^2-q\right) \sum_{m=1}^{\lfloor \frac{n-1}{3} \rfloor} \binom{q}{n-1-m} \mathcal{S}(2, n-1-m, m)\left(q-(n-1-m)\right) \\ & + \left(q^2-q\right) \sum_{m=1}^{\lfloor \frac{n}{3} \rfloor} \binom{q}{n-m} \mathcal{S}(2, n-m, m)\end{aligned}$$

for all $2 \leqslant n < (q-1)/2$, where $\mathcal{S}(2,k,m)$ are the well-known associated Stirling numbers (see [2], and Section 3 below).

2. Carlitz rank of a permutation $\mathcal{P}_s$

Our first aim is to generalize (7) to permutations $\mathcal{P}_n$ with an arbitrary string of poles. It can be seen easily (cf. [3]) that three consecutive poles in $\mathcal{O}_n$ are pairwise distinct, and the poles x_1, x_2 are in $\mathbb{F}_q$. Consequently we obtain $\mathcal{P}_1(x) = \mathcal{F}_1(x)$ and $\mathcal{P}_2(x) = (\mathcal{F}_2(x_2)\mathcal{F}_2(x_1))\mathcal{F}_2(x)$ from (7).

Let $\tau \in S_q$ be a cycle. We denote its length by $l(\tau)$. We write $a \in \mathrm{supp}(\tau)$ if $a \in \mathbb{F}_q$ is not fixed by τ. Suppose the permutation $P_n(x)$ can be decomposed into $F_n(x)$ and m disjoint cycles $\tau_1^{(n)}, \ldots, \tau_m^{(n)}$, i.e.

$$P_n(x) = \tau_1^{(n)} \cdots \tau_m^{(n)} F_n(x), \tag{8}$$

where $l(\tau_j^{(n)}) \geqslant 2$, and $\tau_j^{(n)} = (F_n(x_1^j) \cdots F_n(x_{l_j}^j))$, for $1 \leqslant j \leqslant m$. We remark that $P_n(y) \neq F_n(y)$ if and only if $F_n(y) \in \mathrm{supp}(\tau_j^{(n)})$ for some $1 \leqslant j \leqslant m$. Clearly y must then be in the set $\mathbf{O}_n$. Given a decomposition of P_n of the form (8), we define the set $\bar{\mathbf{O}}_n$ as

$$\bar{\mathbf{O}}_n = \left\{ y \in \mathbf{O}_{n-1} \colon\ F_n(y) \in \mathrm{supp}\left(\tau_j^{(n)}\right) \text{ for some } 1 \leqslant j \leqslant m \right\} \cup \{x_n\}$$

if $x_n \in \mathbb{F}_q$. $\bar{\mathbf{O}}_n$ does not contain x_n if $x_n = \infty$.

From $\bar{P}_n(x) = P_n(x) + a_{n+1}$ we easily see that

$$\bar{P}_n(x) = \bar{\tau}_1^{(n)} \cdots \bar{\tau}_m^{(n)} \bar{F}_n(x)$$

with $\bar{\tau}_j^{(n)} = (\bar{F}_n(x_1^j) \cdots \bar{F}_n(x_{l_j}^j))$, $1 \leqslant j \leqslant m$. It is therefore clear how to decompose $\mathcal{P}_n$ into $\mathcal{F}_n$ and disjoint cycles, provided that we have a method of obtaining the decomposition (8) of P_n from the

decomposition of P_{n-1} of the same nature. We first consider the case $x_{n-1}, x_n \neq \infty$. In Proposition 1 and Theorem 1 below, for a fixed integer j and $k = n-1, n$, the cycle $(F_k(x_1^j)\cdots F_k(x_{l_j}^j))$ is denoted by $\tau_j^{(k)}$.

Proposition 1. *Let $x_{n-1}, x_n \in \mathbb{F}_q$. Suppose that*

$$P_{n-1}(x) = \tau_1^{(n-1)} \cdots \tau_m^{(n-1)} F_{n-1}(x) \tag{9}$$

is a decomposition of $P_{n-1}(x)$ satisfying:

(i) *$\tau_1^{(n-1)}, \ldots, \tau_m^{(n-1)}$ are disjoint cycles.*
(ii) *If $P_{n-1}(x_{n-1}) \neq F_{n-1}(x_{n-1})$ we assume without loss of generality that $F_{n-1}(x_{n-1}) \in \operatorname{supp}(\tau_1^{(n-1)})$ with $x_1^1 = x_{n-1}$, and $l(\tau_j^{(n-1)}) = l_j \geqslant 2$, for $1 \leqslant j \leqslant m$.*
(iii) *If $P_{n-1}(x_{n-1}) = F_{n-1}(x_{n-1})$ we assume without loss of generality that $\tau_1^{(n-1)} = (F_{n-1}(x_{n-1}))$ and $l(\tau_j^{(n-1)}) = l_j \geqslant 2$, for $2 \leqslant j \leqslant m$.*

Then

$$P_n(x) = \big(F_n(x_n)F_n(x_{n-1})\big)\tau_1^{(n)} \cdots \tau_m^{(n)} F_n(x).$$

Proof. We can distinguish three cases:

(1) Suppose that $F_{n-1}(x_n)$ is not in $\operatorname{supp}(\tau_j^{(n-1)})$ for any $j = 1, \ldots, m$ in the decomposition (9), i.e. $x_n \notin \overline{\mathbf{O}}_{n-1}$. In this case we have to show:

(a) If $x \notin \overline{\mathbf{O}}_{n-1}$ and $x \neq x_n$, then $P_n(x) = F_n(x)$.
(b) If $y \in \overline{\mathbf{O}}_{n-1}$ satisfies $y \neq x_{l_1}^1$, and $P_{n-1}(y) = F_{n-1}(y')$, then $P_n(y) = F_n(y')$.
(c) $P_n(x_{l_1}^1) = F_n(x_n)$, and $P_n(x_n) = F_n(x_{n-1})$.

Note that $l_1 = 1$ implies $P_n(x_{n-1}) = F_n(x_n)$ by (c). Otherwise x_{n-1} satisfies the conditions of (b). We give the proofs of (a)–(c), which we will refer to in the other two cases:
If $x \notin \overline{\mathbf{O}}_{n-1}$, then $P_{n-1}(x) = F_{n-1}(x)$. Since $x \neq x_{n-1}, x_n$, we have

$$\begin{aligned} P_n(x) &= \big(P_{n-1}(x) + a_n\big)^{q-2} = \left(\frac{\alpha_{n-2}x + \beta_{n-2}}{\alpha_{n-1}x + \beta_{n-1}} + a_n\right)^{q-2} \\ &= \left(\frac{(a_n\alpha_{n-1} + \alpha_{n-2})x + a_n\beta_{n-1} + \beta_{n-2}}{\alpha_{n-1}x + \beta_{n-1}}\right)^{q-2} \\ &= \left(\frac{\alpha_n x + \beta_n}{\alpha_{n-1}x + \beta_{n-1}}\right)^{q-2} = \frac{\alpha_{n-1}x + \beta_{n-1}}{\alpha_n x + \beta_n} = F_n(x). \end{aligned}$$

This proves part (a). For the proof of part (b), we assume that $P_{n-1}(y) = F_{n-1}(y')$, then

$$\begin{aligned} P_n(y) &= \big(P_{n-1}(y) + a_n\big)^{q-2} = \big(F_{n-1}(y') + a_n\big)^{q-2} \\ &= \left(\frac{\alpha_{n-2}y' + \beta_{n-2}}{\alpha_{n-1}y' + \beta_{n-1}} + a_n\right)^{q-2} = \left(\frac{\alpha_n y' + \beta_n}{\alpha_{n-1}y' + \beta_{n-1}}\right)^{q-2} \\ &= \frac{\alpha_{n-1}y' + \beta_{n-1}}{\alpha_n y' + \beta_n} = F_n(y'). \end{aligned}$$

Finally (c) follows from

$$\begin{aligned}
P_n\left(x_{l_1}^1\right) &= \left(P_{n-1}\left(x_{l_1}^1\right) + a_n\right)^{q-2} = \left(F_{n-1}(x_{n-1}) + a_n\right)^{q-2} \\
&= \left(\frac{\alpha_{n-2}}{\alpha_{n-1}} + a_n\right)^{q-2} = \left(\frac{a_n\alpha_{n-1} + \alpha_{n-2}}{\alpha_{n-1}}\right)^{q-2} \\
&= \frac{\alpha_{n-1}}{\alpha_n} = F_n(x_n) \quad \text{and} \\
P_n(x_n) &= \left(P_{n-1}(x_n) + a_n\right)^{q-2} = \left(F_{n-1}(x_n) + a_n\right)^{q-2} \\
&= \left(\frac{\alpha_{n-2}x_n + \beta_{n-2}}{\alpha_{n-1}x_n + \beta_{n-1}} + a_n\right)^{q-2} \\
&= \left(\frac{(a_n\alpha_{n-1} + \alpha_{n-2})x_n + a_n\beta_{n-1} + \beta_{n-2}}{\alpha_{n-1}x_n + \beta_{n-1}}\right)^{q-2} \\
&= \left(\frac{\alpha_n x_n + \beta_n}{\alpha_{n-1}x_n + \beta_{n-1}}\right)^{q-2} = 0 = F_n(x_{n-1}),
\end{aligned}$$

where in the last step we used

$$F_n(x_{n-1}) = \frac{\alpha_{n-1}x_{n-1} + \beta_{n-1}}{\alpha_n x_{n-1} + \beta_n} = 0.$$

(2) Suppose that $F_{n-1}(x_n)$ is in $\operatorname{supp}(\tau_1^{(n-1)})$, say $x_n = x_r^1$, i.e. $\tau_1^{(n-1)} = (F_{n-1}(x_{n-1}) \cdots F_{n-1}(x_{r-1}^1) F_{n-1}(x_n) \cdots F_{n-1}(x_{l_1}^1))$. In this case we have to show:

(a) If $x \notin \overline{\mathbf{O}}_{n-1}$ then $P_n(x) = F_n(x)$.
(b) If $y \in \overline{\mathbf{O}}_{n-1}$ satisfies $y \neq x_{l_1}^1, x_{r-1}^1$, and $P_{n-1}(y) = F_{n-1}(y')$, then $P_n(y) = F_n(y')$.
(c) $P_n(x_{l_1}^1) = F_n(x_n)$, and $P_n(x_{r-1}^1) = F_n(x_{n-1})$.

Since (a), (b) and the first statement of (c) are shown as in case (1) we only have to show $P_n(x_{r-1}^1) = F_n(x_{n-1})$:

$$\begin{aligned}
P_n\left(x_{r-1}^1\right) &= \left(P_{n-1}\left(x_{r-1}^1\right) + a_n\right)^{q-2} = \left(F_{n-1}(x_n) + a_n\right)^{q-2} \\
&= \left(\frac{\alpha_{n-2}x_n + \beta_{n-2}}{\alpha_{n-1}x_n + \beta_{n-1}} + a_n\right)^{q-2} = \left(\frac{\alpha_n x_n + \beta_n}{\alpha_{n-1}x_n + \beta_{n-1}}\right)^{q-2} \\
&= 0 = F_n(x_{n-1}).
\end{aligned}$$

(3) Finally we suppose that $F_{n-1}(x_n)$ is in the support of a cycle in (9), other than the first one, say in $\operatorname{supp}(\tau_2^{n-1})$ and $x_n = x_s^2$. We have to show:

(a) If $x \notin \overline{\mathbf{O}}_{n-1}$, then $P_n(x) = F_n(x)$.
(b) If $y \in \overline{\mathbf{O}}_{n-1}$ satisfies $y \neq x_{l_1}^1, x_{s-1}^2$, and $P_{n-1}(y) = F_{n-1}(y')$, then $P_n(y) = F_n(y')$.
(c) $P_n(x_{l_1}^1) = F_n(x_n)$, and $P_n(x_{s-1}^2) = F_n(x_{n-1})$.

The proofs are same as that of (a), (b) in case (1) and (c) in case (2). □

The following theorem immediately follows from Proposition 1 in case $\mathcal{P}_n = P_n$, and the remarks preceding Proposition 1, when $\mathcal{P}_n = \bar{P}_n(x)$.

Theorem 1. *Let $x_{n-1}, x_n \in \mathbb{F}_q$. Suppose that*

$$\mathcal{P}_{n-1}(x) = \tau_1^{(n-1)} \cdots \tau_m^{(n-1)} \mathcal{F}_{n-1}(x) \tag{10}$$

is a decomposition of $\mathcal{P}_{n-1}(x)$ satisfying:

(i) $\tau_1^{(n-1)}, \ldots, \tau_m^{(n-1)}$ *are disjoint cycles.*
(ii) *If $\mathcal{P}_{n-1}(x_{n-1}) \neq \mathcal{F}_{n-1}(x_{n-1})$ we assume without loss of generality that $\mathcal{F}_{n-1}(x_{n-1}) \in \operatorname{supp}(\tau_1^{(n-1)})$ with $x_1^1 = x_{n-1}$, and $l(\tau_j^{(n-1)}) = l_j \geqslant 2$, for $1 \leqslant j \leqslant m$.*
(iii) *If $\mathcal{P}_{n-1}(x_{n-1}) = \mathcal{F}_{n-1}(x_{n-1})$ we assume without loss of generality that $\tau_1^{(n-1)} = (\mathcal{F}_{n-1}(x_{n-1}))$ and $l(\tau_j^{(n-1)}) = l_j \geqslant 2$, for $2 \leqslant j \leqslant m$.*

Then $\mathcal{P}_n(x)$ can be decomposed as follows:

(a) *if $x_n \notin \overline{\mathbf{O}}_{n-1}$ then*

$$\mathcal{P}_n(x) = \left(\mathcal{F}_n(x_n)\mathcal{F}_n(x_{n-1}) \cdots \mathcal{F}_n\left(x_{l_1}^1\right)\right)\tau_2^{(n)} \cdots \tau_m^{(n)} \mathcal{F}_n(x), \tag{11}$$

(b) *if $\mathcal{F}_{n-1}(x_n) \in \operatorname{supp}(\tau_1^{(n-1)})$, say $x_n = x_r^1$, then*

$$\mathcal{P}_n(x) = \left(\mathcal{F}_n(x_n)\mathcal{F}_n\left(x_{r+1}^1\right) \cdots \mathcal{F}_n\left(x_{l_1}^1\right)\right)\left(\mathcal{F}_n(x_{n-1})\mathcal{F}_n\left(x_2^1\right) \cdots \mathcal{F}_n\left(x_{r-1}^1\right)\right)\tau_2^{(n)} \cdots \tau_m^{(n)} \mathcal{F}_n(x), \tag{12}$$

(c) *if $\mathcal{F}_{n-1}(x_n) \in \operatorname{supp}(\tau_j^{(n-1)})$, $j \neq 1$, say in $\operatorname{supp}(\tau_2^{(n-1)})$ and $x_n = x_s^2$, then*

$$\mathcal{P}_n(x) = \left(\mathcal{F}_n\left(x_s^2\right)\mathcal{F}_n\left(x_{s+1}^2\right) \cdots \mathcal{F}_n\left(x_{l_2}^2\right)\mathcal{F}_n\left(x_1^2\right) \cdots \mathcal{F}_n\left(x_{s-1}^2\right)\mathcal{F}_n\left(x_1^1\right) \cdots \mathcal{F}_n\left(x_{l_1}^1\right)\right)\tau_3^{(n)} \cdots \tau_m^{(n)} \mathcal{F}_n(x).$$

Next we analyse the case that the last term of the string of poles, i.e. x_n is infinity. Recall that in this case x_{n-1} is in $\mathbb{F}_q$.

Theorem 2. *Suppose P_{n-1} can be decomposed as in* (9). *Assume that for $P_n(x) = (P_{n-1}(x) + a_n)^{q-2}$, $x_n = \infty$. Then*

$$\begin{aligned}
P_n(x) &= \tau_1^{(n)} \cdots \tau_m^{(n)} F_n(x), \quad \text{and for all possible choices of } a_{n+1},\ a_{n+2} \text{ we have} \\
P_{n+1}(x) &= \tau_1^{(n+1)} \cdots \tau_m^{(n+1)} F_{n+1}(x), \quad \text{and} \\
P_{n+2}(x) &= \left(F_{n+2}(x_{n+2})F_{n+2}(x_{n+1})\right)\tau_1^{(n+2)} \cdots \tau_m^{(n+2)} F_{n+2}(x),
\end{aligned}$$

where $\tau_j^{(k)}$ denotes the cycle $(F_k(x_1^j) \cdots F_k(x_{l_j}^j))$ for $k = n-1, n, n+1, n+2$, $1 \leqslant j \leqslant m$.

Proof. To prove the first two equalities it is sufficient to show the following properties:

(a) If $x \notin \overline{\mathbf{O}}_{n-1}$, then $P_n(x) = F_n(x)$ and $P_{n+1}(x) = F_{n+1}(x)$.
(b) If $y \in \overline{\mathbf{O}}_{n-1}$ satisfies $P_{n-1}(y) = F_{n-1}(y')$, then $P_n(y) = F_n(y')$ and $P_{n+1}(y) = F_{n+1}(y')$.

Suppose firstly that $x \notin \overline{\mathbf{O}}_{n-1}$. Then $P_{n-1}(x) = F_{n-1}(x)$, and

$$P_n(x) = \big(P_{n-1}(x) + a_n\big)^{q-2} = \left(\frac{\alpha_{n-2}x + \beta_{n-2}}{\alpha_{n-1}x + \beta_{n-1}} + a_n\right)^{q-2}$$
$$= \left(\frac{(a_n\alpha_{n-1} + \alpha_{n-2})x + a_n\beta_{n-1} + \beta_{n-2}}{\alpha_{n-1}x + \beta_{n-1}}\right)^{q-2}$$
$$= \left(\frac{\alpha_n x + \beta_n}{\alpha_{n-1}x + \beta_{n-1}}\right)^{q-2} = \frac{\alpha_{n-1}x + \beta_{n-1}}{\alpha_n x + \beta_n} = F_n(x).$$

For $x \notin \overline{\mathbf{O}}_{n-1}$ and $x \neq x_{n+1}$ the equality $P_{n+1}(x) = F_{n+1}(x)$ also follows as above. Finally

$$P_{n+1}(x_{n+1}) = \big(P_n(x_{n+1}) + a_n\big)^{q-2} = \left(\frac{\alpha_{n-1}x_{n+1} + \beta_{n-1}}{\alpha_n x_{n+1} + \beta_n} + a_n\right)^{q-2}$$
$$= \left(\frac{(a_n\alpha_n + \alpha_{n-1})x_{n+1} + a_n\beta_n + \beta_{n-1}}{\alpha_n x_{n+1} + \beta_n}\right)^{q-2}$$
$$= \left(\frac{\alpha_{n+1}x_{n+1} + \beta_{n+1}}{\alpha_n x_{n+1} + \beta_n}\right)^{q-2} = 0 = F_{n+1}(x_{n+1}),$$

where in the last step we used $F_{n+1}(x_{n+1}) = \frac{\alpha_n}{\alpha_{n+1}} = 0$.

If $y \in \overline{\mathbf{O}}_{n-1}$ and $P_{n-1}(y) = F_{n-1}(y')$, then

$$P_n(y) = \big(P_{n-1}(y) + a_n\big)^{q-2} = \big(F_{n-1}(y') + a_n\big)^{q-2}$$
$$= \left(\frac{\alpha_{n-2}y' + \beta_{n-2}}{\alpha_{n-1}y' + \beta_{n-1}} + a_n\right)^{q-2} = \left(\frac{\alpha_n y' + \beta_n}{\alpha_{n-1}y' + \beta_{n-1}}\right)^{q-2}$$
$$= \frac{\alpha_{n-1}y' + \beta_{n-1}}{\alpha_n y' + \beta_n} = F_n(y').$$

The identity $P_{n+1}(y) = F_{n+1}(y')$ for $y' \neq x_{n+1}$ follows analogously. Finally for $y' = x_{n+1}$ we obtain

$$P_{n+1}(y) = 0 = F_{n+1}(y')$$

since in this case

$$F_{n+1}(y') = F_{n+1}(x_{n+1}) = \frac{\alpha_n}{\alpha_{n+1}} = 0.$$

The statement for P_{n+2} follows then from Proposition 1. □

Corollary 1. *Let $\mathcal{O}_n = x_1, x_2, \ldots, x_n$ be the string of poles of $\mathcal{P}_n$. If $x_t \neq \infty$, $1 \leqslant t \leqslant n$, then*

$$\mathcal{P}_n(x) = \big(\mathcal{F}_n(x_n)\mathcal{F}_n(x_{n-1})\big)\big(\mathcal{F}_n(x_{n-1})\mathcal{F}_n(x_{n-2})\big)\cdots\big(\mathcal{F}_n(x_2)\mathcal{F}_n(x_1)\big)\mathcal{F}_n(x).$$

If $x_{t_j} = \infty$ for some integers $3 \leqslant t_j \leqslant n$ and $s \leqslant n$ is the largest integer such that $x_{s-1}, x_s \neq \infty$, then

$$\mathcal{P}_n(x) = \big(\mathcal{F}_n(x_s)\mathcal{F}_n(x_{s-1})\big)\cdots\big(\mathcal{F}_n(x_{t_j+2})\mathcal{F}_n(x_{t_j+1})\big)\big(\mathcal{F}_n(x_{t_j-1})\mathcal{F}_n(x_{t_j-2})\big)\cdots\big(\mathcal{F}_n(x_2)\mathcal{F}_n(x_1)\big)\mathcal{F}_n(x).$$

Given a permutation $\mathcal{P}_n$, the string $\mathcal{O}_n$ of poles and the associated rational transformation $\mathcal{R}_n$ can be determined efficiently by the recurrence relation (5). By Theorems 1 and 2 we then have a recursive procedure to decompose $\mathcal{P}_n$ as in (8).

Conversely $\mathcal{P}_n$ can be obtained from $\mathcal{F}_n$ and its string of poles $\mathcal{O}_n$, see [3, Section 5.3], for the case $\mathbf{O}_n \subseteq \mathbb{F}_q$. The method below is a slight extension of that given in [3], which also works in the general case $\mathbf{O}_n \subseteq \mathbb{P}^1(\mathbb{F}_q)$.

Let $\mathcal{R}_n(x) = \frac{ax+b}{cx+d} = \frac{\epsilon ax+\epsilon b}{\epsilon cx+\epsilon d}$, $\epsilon \neq 0$, so that

$$\alpha_{n+1} = \epsilon a, \qquad \beta_{n+1} = \epsilon b, \qquad \alpha_n = \epsilon c, \qquad \beta_n = \epsilon d.$$

We remark that the last pole is then fixed by $x_n = -d/c$ (which is ∞ in the case that $\mathcal{R}_n$ is linear). With Eqs. (5) and (6) for $i = n+1, n, \ldots, 3$ and $x_{i-2} \neq \infty$ we obtain

$$a_i = \frac{\beta_i + x_{i-2}\alpha_i}{\beta_{i-1} + x_{i-2}\alpha_{i-1}}.$$

If $x_{i-2} = \infty$, then $\alpha_{i-2} = 0$ and from $\alpha_i = a_i\alpha_{i-1} + \alpha_{i-2}$ we get $a_i = \alpha_i/\alpha_{i-1}$. Therefore we can recursively calculate a_i and $\alpha_{i-2} = \alpha_i - a_i\alpha_{i-1}$, $\beta_{i-2} = \beta_i - a_i\beta_{i-1}$ for $i = n+1, n, \ldots, 3$. We note that α_i and β_i, $i = 1, 2, \ldots, n-1$, will always be obtained as a multiple of ϵ. Finally from $\alpha_0 = 0$, $\beta_0 = 1$ and $\alpha_2 = a_2\alpha_1 + \alpha_0$ we first obtain $a_2 = \alpha_2/\alpha_1$ and then the identity $\beta_2 = a_2\beta_1 + \beta_0 = a_2\beta_1 + 1$ yields the value for ϵ. Lastly $a_1 = \beta_1$ and $a_0 = \alpha_1$. We remark that in case $x_{n-1} = -b/a$, we get $a_{n+1} = 0$, so that $\mathcal{P}_n(x) = P_n(x)$.

Example 1. Let $q = 17$ and $\mathcal{F}_6$ and $\mathcal{O}_6 = x_1, x_2, x_3, x_4, x_5, x_6$ be prescribed by

$$\mathcal{R}_6 = \frac{3x+1}{2x+3} \quad \text{and} \quad \mathcal{O}_6 = 5, 3, 7, 10, 4, 7.$$

As initial values we then have

$$\alpha_7 = 3\epsilon, \qquad \beta_7 = \epsilon, \qquad \alpha_6 = 2\epsilon, \qquad \beta_6 = 3\epsilon.$$

We obtain recursively

$$a_7 = \frac{\beta_7 + x_5\alpha_7}{\beta_6 + x_5\alpha_6} = 12, \qquad \alpha_5 = \alpha_7 - a_7\alpha_6 = 13\epsilon, \qquad \beta_5 = \beta_7 - a_7\beta_6 = 16\epsilon,$$
$$a_6 = \frac{\beta_6 + x_4\alpha_6}{\beta_5 + x_4\alpha_5} = 4, \qquad \alpha_4 = \alpha_6 - a_6\alpha_5 = \epsilon, \qquad \beta_4 = \beta_6 - a_6\beta_5 = 7\epsilon,$$

and continuing this way we get $a_5 = 4$, $a_4 = a_3 = 12$, $\alpha_3 = 9\epsilon$, $\beta_3 = 5\epsilon$, $\alpha_2 = 12\epsilon$, $\beta_2 = 15\epsilon$, $\alpha_1 = \epsilon$, $\beta_1 = 12\epsilon$. We finally obtain $a_2 = \alpha_2/\alpha_1 = 12$. The equation $\beta_2 = a_2\beta_1 + 1$ yields $15\epsilon = 12 \cdot 12\epsilon + 1$ and therefore $\epsilon = 5$. Hence $a_1 = \beta_1 = 9$, $a_0 = \alpha_1 = 5$, and the permutation $P_6(x)$ is given by

$$P_6(x) = \left(\left(\left(\left((5x+9)^{15} + 12\right)^{15} + 12\right)^{15} + 12\right)^{15} + 4\right)^{15} + 4\Big)^{15} + 12.$$

Now we turn our attention to determining the Carlitz rank of a given permutation $\wp(x)$ of $\mathbb{F}_q$. Clearly linear polynomials are the permutation polynomials of Carlitz rank 0. The set of polynomials $\mathcal{P}_1$ with $a_0 = 1/(b-ad)$, $a_1 = d/(b-ad)$, $a_2 = a$ are in one-to-one correspondence with permutations defined by nonconstant rational linear transformations $(ax+b)/(x+d)$, and hence are precisely the permutations of Carlitz rank 1. In order to study permutations $\wp(x)$ of rank greater than 1, we need the following lemma.

Lemma 1. *Let $\mathcal{P}_n$ and $\mathcal{P}_m$ be two permutations of $\mathbb{F}_q$ with associated rational functions $\mathcal{R}_n(x)$ and $\mathcal{R}_m(x)$, respectively. If $\mathcal{P}_n(x) = \mathcal{P}_m(x)$ for all $x \in \mathbb{F}_q$ and $m+n < q-2$, then $\mathcal{R}_n(x) = \mathcal{R}_m(x)$.*

Proof. Let $\mathcal{F}_n(x)$ and $\mathcal{F}_m(x)$ be the permutations of $\mathbb{F}_q$ induced by $\mathcal{R}_n(x)$ and $\mathcal{R}_m(x)$, respectively. Then $\mathcal{P}_n(x) = \mathcal{F}_n(x)$ and $\mathcal{P}_m(x) = \mathcal{F}_m(x)$ for at least $q-n$ respectively $q-m$ elements of $\mathbb{F}_q$. If $\mathcal{P}_n(x) = \mathcal{P}_m(x)$ for all $x \in \mathbb{F}_q$, then $\mathcal{F}_n(x) = \mathcal{F}_m(x)$ for at least $q-(m+n)$ elements of $\mathbb{F}_q$. Obviously $\mathcal{F}_n(x) = \mathcal{F}_m(x)$ has at most two solutions in $\mathbb{F}_q$ if $\mathcal{F}_n \neq \mathcal{F}_m$. Thus $\mathcal{F}_n(x) = \mathcal{F}_m(x)$ if $q-(m+n) > 2$, which yields the assertion. □

Now that Theorems 1 and 2 enable us to represent a given permutation $\mathcal{P}_n$ as a composition of a rational transformation $\mathcal{F}_n$ and disjoint cycles $\tau_1, \ldots, \tau_m$, a result on the rank of a permutation with such decomposition is in order.

Theorem 3. *Suppose that $\mathcal{P}_s$ can be decomposed as*

$$\mathcal{P}_s(x) = \tau_1 \cdots \tau_m \mathcal{F}_s(x), \tag{13}$$

where $\tau_1, \ldots, \tau_m$ are disjoint cycles of length $l(\tau_j) = l_j \geqslant 2$, $1 \leqslant j \leqslant m$.

(a) *If $\mathcal{F}_s$ is not linear and $\mathcal{F}_s(x_s) \in \operatorname{supp}(\tau_j)$ for some $1 \leqslant j \leqslant m$, then there exists a permutation $\mathcal{P}_n$ with $n = m + \sum_{j=1}^{m} l_j - 1$ such that $\mathcal{P}_s(x) = \mathcal{P}_n(x)$ for all $x \in \mathbb{F}_q$.*
(b) *If $\mathcal{F}_s$ is not linear and $\mathcal{F}_s(x_s) \notin \operatorname{supp}(\tau_j)$ for any $1 \leqslant j \leqslant m$, then there exists a permutation $\mathcal{P}_n$ with $n = m + \sum_{j=1}^{m} l_j + 1$ such that $\mathcal{P}_s(x) = \mathcal{P}_n(x)$ for all $x \in \mathbb{F}_q$.*
(c) *If $\mathcal{F}_s$ is linear then there exists a permutation $\mathcal{P}_n$ with $n = m + \sum_{j=1}^{m} l_j$ such that $\mathcal{P}_s(x) = \mathcal{P}_n(x)$ for all $x \in \mathbb{F}_q$.*

In all three cases, $\operatorname{Crk}(\mathcal{P}_s) = n$ *if* $n < (q-1)/2$.

Proof. Let

$$\begin{aligned}\mathcal{P}_s(x) &= \tau_1 \cdots \tau_m \mathcal{F}_s(x)\\ &= \left(\mathcal{F}_s\left(x_1^1\right) \cdots \mathcal{F}_s\left(x_{l_1}^1\right)\right) \cdots \left(\mathcal{F}_s\left(x_1^m\right) \cdots \mathcal{F}_s\left(x_{l_m}^m\right)\right)\mathcal{F}_s(x).\end{aligned}$$

(a) Without loss of generality we suppose that $x_s = x_1^1$ and we choose $\mathcal{F}_n = \mathcal{F}_s$, which fixes the last pole x_n of $\mathcal{P}_n$ to be x_s. For the string of poles of $\mathcal{P}_n$ we choose

$$\mathcal{O}_n = x_{l_1}^1, \ldots, x_1^1, \ldots, x_{l_m}^m, \ldots, x_1^m, x_1^{m-1}, x_1^{m-2}, \ldots, x_1^1.$$

With the procedure described above, we obtain a permutation $\mathcal{P}_n$ with $n = m + \sum_{j=1}^{m} l_j - 1$. That $\mathcal{P}_n$ has decomposition (13) follows by application of Theorem 1 recursively. Since the first $k = \sum_{j=1}^{m} l_j$ poles of $\mathcal{P}_n$ are distinct, (11) implies after k steps that

$$\mathcal{P}_k(x) = \left(\mathcal{F}_k\left(x_1^m\right) \cdots \mathcal{F}_k\left(x_{l_m}^m\right)\mathcal{F}_k\left(x_1^{m-1}\right) \cdots \mathcal{F}_k\left(x_{l_{m-1}}^{m-1}\right) \cdots \mathcal{F}_k\left(x_1^1\right) \cdots \mathcal{F}_k\left(x_{l_1}^1\right)\right)\mathcal{F}_k(x).$$

The next element $x_1^{m-1} \in \mathcal{O}_n$ is a repeated pole and hence (12) implies:

$$\mathcal{P}_{k+1}(x) = \left(\mathcal{F}_{k+1}\left(x_1^{m-1}\right) \cdots \mathcal{F}_{k+1}\left(x_{l_1}^1\right)\right)\left(\mathcal{F}_{k+1}\left(x_1^m\right) \cdots \mathcal{F}_{k+1}\left(x_{l_m}^m\right)\right)\mathcal{F}_{k+1}(x).$$

The next pole x_1^{m-2} also repeats, therefore the cycle containing $\mathcal{F}_{k+1}(x_1^{m-2})$ splits into two cycles, as described in Theorem 1, part (b). This process yields the decomposition (13) at the nth step.

(b) In this case we again take $\mathcal{F}_n = \mathcal{F}_s$, which fixes the last pole x_n of $\mathcal{P}_n$ to be x_s. With the choice

$$\mathcal{O}_n = x_s, x_{l_1}^1, \ldots, x_1^1, \ldots, x_{l_m}^m, \ldots, x_1^m, x_1^{m-1}, x_1^{m-2}, \ldots, x_1^1, x_s,$$

we obtain $\mathcal{P}_n$ with the cycle structure (13), as in case 1. We note that at the nth step $\mathcal{F}_n(x_s)$ separates to form the trivial cycle $(\mathcal{F}_n(x_s))$.

(c) Again we take $\mathcal{F}_n = \mathcal{F}_s$. For the string of poles we choose

$$\mathcal{O}_n = x_{l_1}^1, \ldots, x_1^1, \ldots, x_{l_m}^m, \ldots, x_1^m, x_1^{m-1}, x_1^{m-2}, \ldots, x_1^1, \infty,$$

and determine the corresponding permutation $\mathcal{P}_n$. After arriving at the decomposition of $\mathcal{P}_{n-1}$ in the form (10), we can apply Theorem 2 to obtain $\mathcal{P}_n$, which has decomposition (13).

The proof of the parts (a)–(c) above demonstrates that starting with a fixed permutation $\mathcal{F}_s$, the procedure we describe yields the smallest n with $\mathcal{P}_n(x) = \mathcal{P}_s(x)$ (and $\mathcal{F}_n(x) = \mathcal{F}_s(x)$) in all three cases. On the other hand if we suppose that there is an integer $n' < n$ such that $\mathcal{P}_{n'}(x) = \mathcal{P}_n(x)$ and $\mathcal{F}_{n'}(x) \neq \mathcal{F}_n(x)$, then by Lemma 1 we have $2n > n + n' \geqslant q - 2$ and hence $n > (q-2)/2$. Consequently in all three cases we have $\mathrm{Crk}(\mathcal{P}_s) = n$ if $n \leqslant (q-2)/2 < (q-1)/2$. □

The following examples demonstrate how (the proof of) Theorem 3 can be used to obtain representations $\mathcal{P}_n$.

Example 2. Let $q = 17$, $\mathcal{R} = \frac{3x+1}{2x+3}$, and $\mathcal{F}$ be the associated permutation. Consider

$$\wp(x) = (10\ 3\ 13)\ (12\ 8)\mathcal{F}(x) = \big(\mathcal{F}(7)\ \mathcal{F}(3)\ \mathcal{F}(5)\big)\ \big(\mathcal{F}(4)\ \mathcal{F}(10)\big)\mathcal{F}(x) = \tau_1\tau_2\mathcal{F}.$$

We observe that 7 is the pole of $\mathcal{R}$ and $\mathcal{F}(7) = 10 \in \mathrm{supp}(\tau_1)$. By Theorem 3(a) we have $\mathrm{Crk}(\wp) = 6$, and following the proof of Theorem 3 we can put $\mathcal{O}_6 = 5, 3, 7, 10, 4, 7$. A representation of this permutation as $\mathcal{P}_6$ has been determined in Example 1.

Example 3. Consider the 5-cycle $(1\ 3\ 5\ 7\ 9) \in S_{17}$. By Theorem 3(c) this permutation has Carlitz rank 6. By putting $\mathcal{O}_6 = 9, 7, 5, 3, 1, \infty$ (as in the proof of Theorem 3), and $\mathcal{F}(x) = x$, our procedure described above (see also Example 1) gives

$$\mathcal{P}_6(x) = \big(\big(\big(\big(\big((x+8)^{15} + 9\big)^{15} + 13\big)^{15} + 1\big)^{15} + 13\big)^{15} + 9\big)^{15} + 1.$$

Similarly, for $(1\ 3\ 5\ 7\ 9)(2\ 6) \in S_{23}$ with Carlitz rank 9, a representation $\mathcal{P}_9$ can be determined by putting $\mathcal{O}_9 = 9, 7, 5, 3, 1, 6, 2, 1, \infty$, and $\mathcal{F}(x) = x$.

3. Counting permutations of Carlitz rank *n*

Let $\mathcal{B}(n)$ be the number of permutations of $\mathbb{F}_q$ with Carlitz rank n. The values of $\mathcal{B}(n)$ can be determined for small n. For values of n up to about half of q, namely for $n < (q-1)/2$ we present formulas expressing $\mathcal{B}(n)$ in terms of $\mathcal{S}(2, k, m)$, the so-called associated Stirling numbers of the first kind.

Clearly we have $\mathcal{B}(0) = q(q-1)$. It is also easy to see that $\mathcal{P}_1(x) = (a_0x + a_1)^{q-2} + a_2 = (a_0'x + a_1')^{q-2} + a_2' = \mathcal{P}_1'(x)$ for all $x \in \mathbb{F}_q$ if and only if $a_i = a_i'$, $i = 0, 1, 2$. Consequently we have $\mathcal{B}(1) = q^2(q-1)$. We recall that the permutations $\mathcal{P}_1$ are precisely all the permutations associated with nonconstant rational transformations $(ax+b)/(x+d)$, $ad - b \neq 0$. As pointed out in [4], the polynomials $\mathcal{P}_2(x) = ((a_0x + a_1)^{q-2} + a_2)^{q-2} + a_3$ and $\mathcal{P}_2'(x) = ((a_0'x + a_1')^{q-2} + a_2')^{q-2} + a_3'$ induce the same permutation if and only if $a_i = a_i'$ for $i = 0, 1, 2, 3$. Thus we have $\mathcal{B}(2) = q^2(q-1)^2$. This property is not valid anymore for $\mathcal{P}_3$. For $u, v \in \mathbb{F}_q^*$, the transposition $(u\ v)$ for instance, can be expressed as $\mathcal{P}_3$ for both choices of $a_0 = -1/(u-v)^2$, $a_1 = -ua_0$, $a_2 = v - u$, $a_3 = 1/(u-v)$, $a_4 = v$, and $a_0' = a_0$, $a_1' = -va_0$, $a_2' = -a_2$, $a_3' = -a_3$, $a_4' = u$ (cf. [4, Remark 3.1]). Evidently a rough upper bound for the total number of permutations of Carlitz rank $n, n < (q-1)/2$, can be given as $\sum_{n=0}^{(q-3)/2} \mathcal{B}(n) \leqslant q(q-1) + q^2((q-1)^{(q-1)/2} - q + 1)/(q-2)$, the right-hand side being the number of formal expressions of the form $\mathcal{P}_s$, $s \leqslant (q-3)/2$. Therefore the majority of the $q!$ permutations of $\mathbb{F}_q$

have Carlitz rank $\geqslant (q-1)/2$. The following theorem shows that small polynomial degree implies large Carlitz rank.

Theorem 4. *Let $g(x)$ be a permutation polynomial in $\mathbb{F}_q[x]$ with $\deg(g) = d > 1$ and suppose that $\mathrm{Crk}(g) = n$. Then*

$$n \geqslant q - 1 - d.$$

Proof. For $\mathcal{P}_n$ satisfying $g(x) = \mathcal{P}_n(x)$ for all $x \in \mathbb{F}_q$, let $\mathcal{R}_n = (\alpha_{n+1}x + \beta_{n+1})/(\alpha_n x + \beta_n)$ be its rational convergent, and $\mathcal{F}_n$ be the associated permutation. Then $g(x) \neq \mathcal{F}_n(x)$ for at most n elements $x \in \mathbb{F}_q$. We note by Theorem 3, that $g(x)$ and $\mathcal{F}_n(x)$ differ at exactly n elements if and only if $\mathcal{P}_n = \tau\mathcal{F}_n$ for an n-cycle τ containing $\mathcal{F}_n(-\beta_n/\alpha_n)$. If $\mathcal{F}_n$ is not linear, the polynomial $g(x)(\alpha_n x + \beta_n) - (\alpha_{n+1}x + \beta_{n+1})$ of degree $d+1$ has at least $q-n$ solutions which yields the assertion. If $\mathcal{F}_n$ is linear then the polynomial $\beta_n g(x) - (\alpha_{n+1}x + \beta_{n+1})$ of degree d has more than $q-n$ solutions, which again proves the claim. □

We now recall the associated Stirling numbers of the first kind. Let t, k, m be integers with $t, k \geqslant 1$, $m \geqslant 0$. Consider the set $s(t,k,m)$ of permutations $\pi \in S_k$ with cycle decomposition $\pi = \tau_1 \cdots \tau_m$, such that $l(\tau_i) \geqslant t$, for $i = 1, 2, \ldots, m$. The numbers defined as $\mathcal{S}(t,k,m) = |s(t,k,m)|$ are called associated Stirling numbers of the first kind (see, for instance, [2] and [7, id:A008306]). In other words $\mathcal{S}(t,k,m)$ denotes the number of ways of arranging k objects into m cycles, each cycle being of length $\geqslant t$. We will be using $\mathcal{S}(2,k,m)$, the number of permutations in S_k which have m cycles and no fixed points. The associated Stirling numbers $\mathcal{S}(2,k,m)$ satisfies the recurrence relation

$$\mathcal{S}(2, k+1, m+1) = k\mathcal{S}(2, k, m+1) + k\mathcal{S}(2, k-1, m) \tag{14}$$

(with obvious starting values).

Theorem 3 enables us to derive formulas for $\mathcal{B}(n)$, $n < (q-1)/2$, involving $\mathcal{S}(2,k,m)$. Therefore the explicit calculation of $\mathcal{B}(n)$ requires the calculation of the numbers $\mathcal{S}(2,k,m)$ by (14).

Theorem 5. *The number $\mathcal{B}(n)$ of permutations of $\mathbb{F}_q$ with Carlitz rank n is given by*

$$\begin{aligned}\mathcal{B}(n) = {} & \left(q^2 - q\right) \sum_{m=1}^{\lfloor \frac{n+1}{3} \rfloor} \binom{q}{n+1-m} \mathcal{S}(2, n+1-m, m)(n+1-m) \\ & + \left(q^2 - q\right) \sum_{m=1}^{\lfloor \frac{n-1}{3} \rfloor} \binom{q}{n-1-m} \mathcal{S}(2, n-1-m, m)\left(q - (n-1-m)\right) \\ & + \left(q^2 - q\right) \sum_{m=1}^{\lfloor \frac{n}{3} \rfloor} \binom{q}{n-m} \mathcal{S}(2, n-m, m)\end{aligned}$$

for all $2 \leqslant n < (q-1)/2$.

Proof. Let $\wp(x) = \mathcal{P}_n(x)$ be a permutation of Carlitz rank $n < (q-1)/2$. By the proof of Theorem 3 we have a unique decomposition of $\wp(x)$

$$\wp(x) = \tau_1 \cdots \tau_m F(x) \tag{15}$$

as a product of a permutation $F(x) = (ax+b)/(x+d)$ for $x \neq -d$ and $F(-d) = a$, and m disjoint cycles with $l(\tau_j) = l_j \geqslant 2$, $1 \leqslant j \leqslant m$. Theorem 3 also shows that the integers n, m satisfy $n = m + \sum_{j=1}^{m} l_j + \delta$,

where $\delta \in \{0, 1, -1\}$. These three values of δ arise in relation with the three cases below. We enumerate the permutations (15), which emerge from each of these cases, and their sum gives $\mathcal{B}(n)$.

First we count the permutations of Carlitz rank n for which $F(x)$ in (15) is nonlinear and $F(-d) = a$ is contained in one of the cycles τ_j, $1 \leqslant j \leqslant m$. In this case $m + \sum_{j=1}^{m} l_j - 1 = n$, i.e. the m cycles altogether contain $n + 1 - m$ elements. Since $l_j \geqslant 2$ for $1 \leqslant j \leqslant m$, we have $2m \leqslant \sum_{j=1}^{m} l_j$, i.e. $1 \leqslant m \leqslant (n+1)/3$. For each m in this range the number of possible products $\tau_1 \cdots \tau_m$ is $\binom{q}{n+1-m}\mathcal{S}(2, n + 1 - m, m)$. As for $F(x)$, there are $(q^2 - q)(n + 1 - m)$ choices: d can be any element of $\mathbb{F}_q$, there are $n + 1 - m$ choices for a, as a has to be in one of the m cycles, and for each choice of the pair a, d there are $q - 1$ choices for b, so that $ad - b \neq 0$. Summing over m we have a total of

$$\left(q^2 - q\right) \sum_{m=1}^{\lfloor \frac{n+1}{3} \rfloor} \binom{q}{n+1-m} \mathcal{S}(2, n + 1 - m, m)(n + 1 - m)$$

permutations.

Next we count the permutations in (15), where $F(x)$ is nonlinear and $F(-d) = a$ is not in $\operatorname{supp}(\tau_j)$ for any $1 \leqslant j \leqslant m$. In this case $n = m + \sum_{j=1}^{m} l_j + 1$, i.e. the m cycles contain altogether $n - 1 - m$ elements. For each m, $1 \leqslant m \leqslant (n-1)/3$, we have precisely $\binom{q}{n-1-m}\mathcal{S}(2, n - 1 - m, m)$ choices for the products $\tau_1 \cdots \tau_m$. Each of them can be combined with $(q^2 - q)(q - (n - 1 - m))$ permutations $F(x)$ since we have q choices for d, a must be among the $q - (n - 1 - m)$ elements, not contained in any of the m cycles, and again for each pair a, d we have $q - 1$ choices for b. Summing over m we obtain

$$\left(q^2 - q\right) \sum_{m=1}^{\lfloor \frac{n-1}{3} \rfloor} \binom{q}{n-1-m} \mathcal{S}(2, n - 1 - m, m)\left(q - (n - 1 - m)\right)$$

permutations.

Finally we count the permutations for which $F(x)$ in (15) is linear. Then the m cycles in (15) contain exactly $n - m$ elements. Considering that there are $q^2 - q$ linear polynomials and summing over m, $1 \leqslant m \leqslant n/3$, we obtain

$$\left(q^2 - q\right) \sum_{m=1}^{\lfloor \frac{n}{3} \rfloor} \binom{q}{n-m} \mathcal{S}(2, n - m, m)$$

for the number of permutations of this type. □

It is easy to calculate $\mathcal{B}(n)$ for small n:

$$\mathcal{B}(0) = q(q-1), \qquad \mathcal{B}(1) = q^2(q-1), \qquad \mathcal{B}(2) = q^2(q-1)^2,$$

$$\mathcal{B}(3) = \frac{1}{2}q^2(q-1)^2(2q-3), \qquad \mathcal{B}(4) = \frac{1}{6}q^2(q-1)^2(q-2)(6q-13),$$

$$\mathcal{B}(5) = \frac{1}{12}q^2(q-1)^2(q-2)(q-3)(12q-35),$$

$$\mathcal{B}(6) = \frac{1}{120}q^2(q-1)^2(q-2)(q-3)\left(120q^2 - 926q + 1799\right),$$

$$\mathcal{B}(7) = \frac{1}{120}q^2(q-1)^2(q-2)(q-3)(q-4)\left(120q^2 - 1146q + 2765\right),$$

$$\mathcal{B}(8) = \frac{1}{1260}q^2(q-1)^2(q-2)(q-3)(q-4)(q-5)\left(1260q^2 - 14\,373q + 41\,473\right),$$

$$\mathcal{B}(9) = \frac{1}{5040}q^2(q-1)^2(q-2)(q-3)(q-4)(q-5)\big(5040q^3 - 97\,182q^2 + 626\,590q - 1\,349\,523\big),$$

$$\mathcal{B}(10) = \frac{1}{10\,080}q^2(q-1)^2(q-2)(q-3)(q-4)(q-5)(q-6) \times \big(10\,080q^3 - 223\,484q^2 + 1\,657\,175q - 4\,106\,319\big).$$

The reader will immediately notice that the expressions above exhibit the following pattern for $n > 3$:

if $n \equiv 0 \pmod 3$, then $\mathcal{B}(n) = q^2(q-1)^2(q-2)\cdots(q-(2n-3)/3)f_n(q)$,
if $n \equiv 1 \pmod 3$, then $\mathcal{B}(n) = q^2(q-1)^2(q-2)\cdots(q-(2n-2)/3)g_n(q)$,
if $n \equiv 2 \pmod 3$, then $\mathcal{B}(n) = q^2(q-1)^2(q-2)\cdots(q-(2n-1)/3)h_n(q)$

where f_n, g_n, h_n are monic polynomials of degree $\lfloor \frac{n}{3} \rfloor$. This behaviour can be easily explained through a careful inspection of the formula giving $\mathcal{B}(n)$.

One may also be interested in bounds for the maximum value $\mathrm{Crk}_M(q)$, of the Carlitz rank that a permutation of $\mathbb{F}_q$ can have. A lower bound for $\mathrm{Crk}_M(q)$ follows from Theorem 4. Let $\delta > 1$ be the smallest integer satisfying $\gcd(\delta, q-1) = 1$. Then $\mathrm{Crk}_M(q) \geqslant q - 1 - \delta$.

By a judicious choice of $\wp(x)$ and $F(x)$ in (15), one can also obtain the following upper bound. Let $\wp(x)$ be a nonlinear permutation with $\wp(0) = y_0$ and $\wp(1) = y_1$. If we put $F(x) = (y_1 - y_0)x + y_0$ then $F(x) = \wp(x)$ if $x = 0, 1$. Consequently $\wp(x)$ can be written as $\tau_1\tau_2\cdots\tau_m F(x)$ with at most $q-2$ elements arranged into the cycles $\tau_1, \tau_2, \ldots, \tau_m$. Then $m \leqslant (q-3)/2$ and hence $\mathrm{Crk}_M(q) \leqslant (q-3)/2 + q - 2 = (3q-7)/2$.

4. Remarks

Permutation polynomials with specific properties are needed for various applications of finite fields. In particular permutation polynomials with given cycle structure are of interest, and our results presented in Section 2 yield a method to construct such polynomials. When τ is a given permutation with $\tau = \tau_1 \cdots \tau_m$, such that τ_i for $i = 1, 2, \ldots, m$ are disjoint cycles satisfying $n = \mathrm{supp}(\tau) + m < (q-1)/2$, it is straightforward to determine a polynomial $\mathcal{P}_n$ representing τ, see Example 3. The polynomial $\mathcal{P}_n$ is not unique, however, by Theorem 3 no $\mathcal{P}_s$, $s < n$ can represent τ.

Our results stated in Theorems 3 and 5, which concern evaluating $\mathrm{Crk}(\mathcal{P}_s) = n$ and $\mathcal{B}(n)$ are valid only for $n < (q-1)/2$. It would be interesting to extend these results, at least to obtain bounds for $\mathcal{B}(n)$ when $n \geqslant (q-1)/2$.

Results of this paper can be used to construct pseudorandom sequences with long periods by imposing suitable conditions on the polynomials $\mathcal{P}_n$. Work on this topic is in progress.

References

[1] L. Carlitz, Permutations in a finite field, Proc. Amer. Math. Soc. 4 (1953) 538.
[2] L. Comtet, Advanced Combinatorics, the Art of Finite and Infinite Expansions, Reidel, Dordrecht, 1974.
[3] A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, On the cycle structure of permutation polynomials, Finite Fields Appl. 14 (2008) 593–614.
[4] A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, Enumeration of a class of sequences generated by inversions, in: Proceedings of the First Int. Workshop on Coding and Cryptology, Fujian, China, June 2007, in: Ser. Coding Theory Cryptol., vol. 4, World Sci. Publ., Singapore, 2008.
[5] R. Lidl, H. Niederreiter, Finite Fields, second ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.
[6] I.E. Shparlinski, Finite Fields: Theory and Computation. The Meeting Point of Number Theory, Computer Science, Coding Theory and Cryptography, Math. Appl., vol. 477, Kluwer Acad. Publ., Dordrecht, 1999.
[7] N.J. Sloane, On-line Encyclopedia of integer sequences, published electronically at http://www.research.att.com/~njas/sequences.